**Majalah Ilmiah Matematika dan Statistika Volume 19 Nomor 2, 2019, 95 – 103**
*https://jurnal.unej.ac.id/index.php/MIMS/index* ISSN 1411-6669

# PENGAMANAN *POLYALPHABETIC* DENGAN *AFFINE CIPHER* BERDASARKAN BARISAN FIBONACCI

**(*Polyalphabetic Security with Affine Cipher Based on Fibonacci Sequence*)**

**Lestari Fidi Astuti, Kiswara Agung Santoso, Ahmad Kamsyakawuni**

Jurusan Matematika, Fakultas MIPA, Universitas Jember
Jl. Kalimantan 37 Jember 68121, Indonesia
Email: lestarifidi15@gmail.com, {kiswara, kamsyakawuni}.fmipa@unej.ac.id

**Abstract.** Affine cipher is a classic cryptographic algorithm substitution technique. Substitution technique is the encryption process for every character in the plaintext will be subtituted by another character. Affine cipher uses two types of keys. Each character of plaintext to be encrypted substituted by the same key. This research discusses about modify one of the key affine cipher, to produce a different key that will be substituted with each plaintext character. Key modifications are made by the Fibonacci sequence rules. This study also compares affine cipher and key modification affine cipher by finding corelation coeffiecient values. The results obtained from the comparison of the two algorithms, encryption that uses affine cipher key modification is better than affine cipher.

**Keywords:** Cryptography, Affine Cipher, Fibonacci, Correlation Value
**MSC 2010:** 1648

## 1. Pendahuluan

Perkembangan teknologi informasi yang semakin canggih memberikan perubahan yang besar terhadap kehidupan manusia. Saat ini berbagai macam kegiatan manusia dibantu dengan teknologi salah satunya dalam bidang komunikasi. Dalam komunikasi sangat penting menjaga keamanan pengiriman pesan untuk menjaga privasi seseorang. Keamanan pengiriman pesan dapat menerapkan ilmu kriptografi. Ilmu kriptografi merupakan ilmu ataupun seni yang mempelajari tentang menjaga keamanan pengiriman pesan dari seseorang yang ditujukan ke orang lain. Pesan asli yang akan dikirim disebut dengan *plaintext*, sedangkan pesan hasil dari pengkodean disebut dengan *ciphertext*. Enkripsi adalah proses mengubah *plaintext* menggunakan kode rahasia sehingga menghasilkan *ciphertext*. Dekripsi adalah proses mengubah *cipertext* ke bentuk aslinya dengan menggunakan kode rahasia.

*Affine cipher* merupakan salah satu algoritma kriptografi klasik teknik substitusi. *Affine cipher* menggunakan dua jenis kunci yaitu, kunci bilangan relatif prima dan bilangan bulat untuk penggeser [6]. Kekuatan algoritma *affine cipher* terletak pada kunci yang

digunakan. *Affine cipher* merupakan algoritma yang paling baik dari algoritma substitusi lainnya, karena kunci penggeser dapat menggunakan barisan tertentu. Barisan adalah bilangan yang membentuk suatu pola urutan tertentu. Terdapat beberapa macam barisan salah satunya Barisan Fibonacci. Barisan Fibonacci merupakan suatu urutan bilangan dimana nilai suku selanjutnya merupakan jumlah dua suku sebelumnya [3].

Beberapa artikel penelitian sebelummya yang berhubungan dengan *affine cipher*, yaitu dengan judul *Encryption of Hindi plaintext Using Modifited Affine cipher Technique* membahas tentang penerapan algoritma *affine cipher* dengan *plaintext* berupa karakter huruf india [4]. *Modification affine cipher algorithm for cryptography password* membahas tentang modifikasi pada *plaintext*, dimana sebelum melakukan enkripsi dan dekripsi posisi *plaintext* dibalik, sehingga karakter pertama berada di posisi terakhir [5]. *Aplikasi Kriptografi Komposisi One Time Pad Cipher dan Affine Cipher* membahas tentang proses enkripsi menggunakan *one time pad cipher* dengan kunci berdasarkan barisan Fibonacci, selanjutnya hasil *ciphertext* tersebut dienkripsi dengan *affine cipher* [2]. Peneliti akan menggunakan algoritma *affine cipher* untuk keamanan pengiriman pesan teks dengan modifikasi kunci pada kunci penggeser. Pengirim pesan memberikan dua jenis kunci kepada penerima yaitu, kunci bilangan yang relatif prima sebagai pengali dan kunci penggeser berupa teks. Penerima pesan melakukan pembentukan pada kunci penggeser dengan aturan barisan Fibonacci untuk melakukan proses dekripsi sehingga menghasilkan pesan asli. Penelitian ini bertujuan untuk menerapkan algoritma *affine cipher* dengan modifikasi kunci berdasarkan barisan Fibonacci pada keamanan pengiriman pesan teks, Mengetahui algoritma yang lebih baik antara *affine cipher* dan *affine cipher* modifikasi kunci berdasarkan barisan Fibonacci serta membuat program dengan algoritma tersebut.

## 2. Metodologi

Penelitian ini menggunakan data berupa teks. Teks tersebut dapat berupa karakter alfabet, angka, simbol, dan tanda spasi yang terdapat dalam *printable* ASCII. Data yang digunakan akan dikonversi ke bentuk desimal menggunakan tabel ASCII sebelum proses enkripsi atau dekripsi.

**Enkripsi**

Terdapat beberapa tahapan dalam proses enkripsi, yaitu:

a. Konversi *Plaintext*

Pada langkah ini *plaintext* yang akan melalui proses enkripsi dikonversi terlebih dahulu kedalam bentuk desimal menggunakan tabel ASCII.

b. Pembentukan Kunci

Kunci terdiri dari dua jenis yaitu, kunci bilangan relatif prima sebagai pengali dan kunci pengeser berupa teks. Kunci penggeser yang akan digunakan harus dikonversi terlebih dahulu ke bentuk desimal. Pembentukan kunci penggeser dilakukan dengan menjumlahkan semua karakter dari kunci penggeser. Selanjutnya, pembentukan kunci dilakukan menggunakan aturan barisan Fibonacci dan jumlah karakter yang digunakan adalah 95, secara sistematis didapat Persamaan (1).

$$F(n) = F(n - 1) + F(n – 2) \bmod 95 \quad (1)$$

c. Proses Enkripsi

Poses enkripsi pesan dilakukan menggunakan algoritma *affine cipher* dengan modifikasi kunci berdasarkan barisan Fibonacci. Algoritma ini memiliki dua kunci yaitu, kunci *a* merupakan bilangan yang relatif prima dan kunci *b* sebagai kunci penggeser berupa teks. Hasil pembentukan kunci yang telah dilakukan merupakan kunci penggeser dari algoritma ini. Setiap karakter *plaintext* memiliki kunci penggeser yang berbeda-beda. Proses enkripsi dilakukan dengan menggunakan Persaaman (2).

$$C_i = ((a(P_i – 32) + b_i) \bmod 95) + 32 \quad (2)$$

**Dekripsi**

Terdapat beberapa tahapan dalam proses dekripsi, yaitu:

a. Konversi *Ciphertext*

*Ciphertext* yang akan didekripsi dikonversi terlebih dahulu kedalam bentuk desimal

b. Pembentukan Kunci

Pada langkah ini pembentukan kunci yang akan dilakukan sama dengan pembentukan kunci pada proses enkripsi. Sehingga kunci yang digunakan pada proses enkripsi dan dekripsi adalah kunci yang sama (kunci tunggal). Selain itu, pada tahap ini dilakukan pencarian terhadap invers dari kunci bilangan yang relatif prima ($a^{-1}$).

c. Proses Dekripsi

Pada tahap ini dilakukan untuk mengubah *ciphertext* menjadi *plaintext.* Proses dekripsi dilakukan dengan menggunakan persaaman (3).

$$P_i = (a^{-1}((C_i – 32) – b_i) \bmod 95) + 32 \quad (3)$$

**Analisi Koefisien Korelasi**

Perhitungan koefisien korelasi *plaintext* dan *cipertext* bertujuan untuk mengetahui hubungan linier antara *plaintext* dan *ciphertext* tersebut. Jika nilai korelasi yang dihasilkan 1 atau -1 maka memiliki hubungan linier yang kuat antara *plaintext* dan *ciphertext* . Dalam kriptografi hal ini merupakan enkripsi yang tidak baik. Jika korelasi bernilai 0 maka *plaintext* dan *ciphertext* tidak memiliki hubungan linear sehingga algoritma kriptografi memiliki proses enkripsi yang baik [6].

Perhitungan nilai korelasi dilakukan dengan menggunakan persamaan berikut.

$$KK(x,y) = \frac{\sum_{i=1}^{n}\big(x_i - \mu(x)\big)\big(y_i - \mu(y)\big)}{\sigma(x)\sigma(y)} \quad (4)$$

dengan:

$$\mu(x) = \frac{1}{n}\sum_{i=1}^{n} x_i \quad \text{dan} \quad \mu(y) = \frac{1}{n}\sum_{i=1}^{n} y_i$$

$$\sigma(x) = \sqrt{\sum_{i=1}^{n}(x_i - \mu(x))^2} \quad \text{dan} \quad \sigma(y) = \sqrt{\sum_{i=1}^{n}(y_i - \mu(y))^2}$$

## 3. Hasil dan Pembahasan

**Enkripsi *Affine Cipher* dengan Modifikasi Kunci Berdasarkan Barisan Fibonacci**

Proses enkripsi dilakukan dengan menginputkan *plaintext* dan 2 jenis kunci yaitu, kunci *a* berupa bilangan yang relatif prima dengan 95 dan kunci *b* berupa teks. *Plaintext* dienkripsi dengan kedua kunci tersebut sehingga menghasilkan *ciphertext* yang acak dan tidak berpola seperti pada Tabel 1.

Tabel 1. Contoh hasil enkripsi

| | | |
|---|---|---|
| *Plaintext* | : | Ini password yang digunakan: LFA@123ebfm |
| Kunci *a* | : | 3 |
| Kunci *b* | : | lestari |
| *ciphertext* | : | 8H5s>d'f>1p(2yCv 3*LB{qdHi6=8,2ie}e3yJ?v |

Beberapa tahapan yang harus dilakukan untuk menghasilkan *ciphertext*, yaitu:

a. Konversi *Plaintext*

Pada tahap ini, *plaintext* yang akan melalui proses enkripsi harus dikonversi terlebih dahulu ke dalam bentuk desimal menggunakan tabel ASCII seperti pada Tabel 2.

Tabel 2. Konversi *plaintext* ke desimal

| $P_i$ | | Desimal |
|---|---|---|
| I | : | 73 |
| n | : | 110 |
| i | : | 105 |
| *Spc* | : | 32 |
| . | . | . |
| . | . | . |
| b | : | 98 |
| f | : | 102 |
| m | : | 109 |

b. Pembentukan Kunci

Tahap ini dilakukan pembentukan pada kunci *b* berupa teks, dimana pembentukan kunci tersebut mengikuti aturan barisan Fibonacci. Misalkan kunci *b* yang digunakan adalah "lestari". Pembentukan kunci dilakukan dengan cara menjumlahkan semua karakter dari kata "lestari" dan dimodulo 95. Karakter tersebut dikonversi ke desimal meggunakan tabel ASCII seperti pada Tabel 3. Selanjutnya dilakukan perhitungan dengan menggunakan Persamaan (1). Hasil dari permbentukan kunci seperti yang terlihat pada Gambar 1.

Tabel 3. Konversi kunci ke desimal

| Kunci | l | e | s | t | a | r | i |
|---|---|---|---|---|---|---|---|
| Desimal | 108 | 101 | 115 | 116 | 97 | 114 | 105 |
| Jumlah | 756 | mod | 95 | = | 91 | | |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 91 | 91 | 87 | 83 | 75 | 63 | 43 | 11 | 54 | 65 |
| 24 | 89 | 18 | 12 | 30 | 42 | 72 | 19 | 91 | 15 |
| 11 | 26 | 37 | 63 | 5 | 68 | 73 | 46 | 24 | 70 |
| 94 | 69 | 68 | 42 | 15 | 57 | 72 | 34 | 11 | 45 |

Gambar 1. Pembentukan kunci

c. Proses Enkripsi

Proses enkripsi dilakukan menggunakan *affine cipher* dengan modifikasi kunci berdasarkan barisan Fibonacci. Kunci *a* yang digunakan dalam contoh ini adalah 3 dan kunci *b* yang digunakan adalah hasil pembentukan kunci seperti pada Gambar 1. *Plaintext* dan dua jenis kunci yang telah diinputkan akan dienkripsi dengan menggunakan Persamaan (2) sehingga didapatkan perhitungan sebagai berikut.

$$C_i = \left((a(P_i - 32) + b_i) mod\ 95\right) + 32$$

$$\begin{aligned}
\boldsymbol{C_1} &= \left((3(73-32) + \mathbf{91}) mod\ 95\right) + 32 \\
&= \left((3.41 + \mathbf{91}) mod\ 95\right) + 32 \\
&= \left((123 + \mathbf{91}) mod\ 95\right) + 32 \\
&= (214\ mod\ 95) + 32 \\
&= 24 + 32 \\
&= 54\ \textbf{(8)}
\end{aligned}$$

$$\begin{aligned}
\boldsymbol{C_2} &= \left((3(110-32) + \mathbf{91}) mod\ 95\right) + 32 \\
&= \left((3.78 + \mathbf{91}) mod\ 95\right) + 32 \\
&= \left((234 + \mathbf{91}) mod\ 95\right) + 32 \\
&= (325\ mod\ 95) + 32 \\
&= 40 + 32 \\
&= 72\ \textbf{(H)}
\end{aligned}$$

$$\begin{aligned}
\boldsymbol{C_4} &= \left((3(32-32) + \mathbf{83}) mod\ 95\right) + 32 \\
&= \left((3.0 + \mathbf{83}) mod\ 95\right) + 32 \\
&= \left((0 + \mathbf{83}) mod\ 95\right) + 32 \\
&= (83\ mod\ 95) + 32 \\
&= 83 + 32 \\
&= 115\textbf{(s)} \\
&\ \ . \\
&\ \ . \\
&\ \ .
\end{aligned}$$

$$\begin{aligned}
\boldsymbol{C_{40}} &= \left((3(109-32) + \mathbf{45}) mod\ 95\right) + 32 \\
&= \left((3.77 + \mathbf{45}) mod\ 95\right) + 32 \\
&= \left((231 + \mathbf{45}) mod\ 95\right) + 32 \\
&= (276\ mod\ 95) + 32
\end{aligned}$$

$C_3$ = $((3(105-32)+\mathbf{87}) mod\ 95)+32$ = *86 + 32*
= $((3.73+\mathbf{87}) mod\ 95)+32$ = *118* ***(v)***
= $((219+\mathbf{87}) mod\ 95)+32$
= $(306\ mod\ 95)+32$
= *21 + 32*
= *53* ***(5)***

Semua karakter dalam *plaintext* menggunakan kunci *a* yang sama, sedangkan untuk setiap karakter dalam *plaintext* menggunakan kunci *b* yang berbeda yaitu, $P_1$ dengan $b_1$, $P_2$ dengan $b_2$ dan seterusnya. Perhitungan tersebut menghasilkan *ciphertext* **8H5s>d'f>1p(2yCv 3*LB{qdHi6=8,2ie}e3yJ?v**

**Dekripsi *Affine Cipher* dengan Modifikasi Kunci Berdasarkan Barisan Fibonacci**

Proses dekripsi dilakukan dengan menginputkan *ciphertext* dan 2 jenis kunci yaitu, kunci *a* berupa invers perkalian bilangan relatif prima yang digunakan dan kunci *b* berupa teks. *Ciphertext* didekripsi dengan kedua kunci tersebut sehingga mengghasilkan *plaintext*. Beberapa tahapan yang harus dilakukan untuk mendapatkan *plaintext* sebagai berikut.

a. Konversi *Ciphertext*

Pada tahap ini, *Ciphertext* yang akan melalui proses dekripsi harus dikonversiterlebih dahulu ke dalam bentuk desimal menggunakan tabel ASCII.

Tabel 4. Konversi *ciphertext* ke desimal

| $P_i$ | | Desimal |
|---|---|---|
| 8 | : | 56 |
| H | : | 72 |
| 5 | : | 53 |
| s | : | 115 |
| . | . | . |
| | . | . |
| J | : | 74 |
| ? | : | 63 |
| v | : | 118 |

b. Pembentukan Kunci

Pembentukan kunci *b* pada proses dekripsi sama dengan pembentukan kunci pada proses enkripsi seperti yang terlihat pada Gambar 1. Selain itu, pada tahap ini dilakukan pencarian invers perkalian dari kunci *a* dengan mengunakan perluasan algoritma *Euclidean*

Mencari invers dari 3 *mod* 95

95 = 3.31+2 $\Rightarrow$ 2 = 95-3.31 (4)
3 = 2.1+1 $\Rightarrow$ 1 = 3-2.1 (5)

2 = 1.2+0

Substitusikan persamaan (4) ke (5)

1 = 3 – (95 – 3.31) . 1
1 = 3 + 95.1 + 3.31
1 = 3.32 + 95.1

Dari persamaan terakhir di atas diperoleh 32 adalah invers dari 3 *mod* 95.

c. Proses Dekripsi

Proses dekripsi dilakukan menggunakan *affine cipher* dengan modifikasi kunci berdasarkan barisan Fibonacci. Kunci *a* yang digunakan dalam contoh ini adalah 32 dan kunci *b* yang digunakan merupakan hasil pembentukan kunci seperti pada Gambar 1. *Ciphertext* dan dua jenis kunci yang telah diinputkan akan didekripsi dengan menggunakan Persamaan (3) sehingga didapatkan perhitungan sebagai berikut.

$P_i = (a^{-1}((C_i - 32) - b_i) mod 95) + 32$

$\boldsymbol{P_i} = \big(32\big((56 - 32) - \mathbf{91}\big) mod\ 95\big) + 32$
$= (32(24 - \mathbf{91}) mod\ 95) + 32$
$= (32(-67) mod\ 95) + 32$
$= (-2144\ mod\ 95) + 32$
$= 41 + 32$
$= 73$ ***(I)***

$\boldsymbol{P_2} = \big(32\big((72 - 32) - \mathbf{91}\big) mod\ 95\big) + 32$
$= (32(40 - \mathbf{91}) mod\ 95) + 32$
$= (32(-51) mod\ 95) + 32$
$= (-1632\ mod\ 95) + 32$
$= 78 + 32$
$= 110$ ***(n)***

$\boldsymbol{P_3} = \big(32\big((53 - 32) - \mathbf{87}\big) mod\ 95\big) + 32$
$= (32(21 - \mathbf{87}) mod\ 95) + 32$
$= (32(-66) mod\ 95) + 32$
$= (-2112\ mod\ 95) + 32$
$= 73 + 32$
$= 105$ ***(i)***

$\boldsymbol{P_4} = \big(32\big((115 - 32) - \mathbf{83}\big) mod\ 95\big) + 32$
$= (32(83 - \mathbf{83}) mod\ 95) + 32$
$= (32(0) mod\ 95) + 32$
$= (0\ mod\ 95) + 32$
$= 0 + 32$
$= 32$***(spc)***

.
.
.

$\boldsymbol{P_{40}} = \big(32\big((118 - 32) - \mathbf{45}\big) mod\ 95\big) + 32$
$= (32(86 - \mathbf{45}) mod\ 95) + 32$
$= (32(41) mod\ 95) + 32$
$= (1312\ mod 95) + 32$
$= 77 + 32$
$= 109$***(m)***

Semua karakter dalam *ciphertext* menggunakan kunci *a* yang sama, sedangkan untuk setiap karakter dalam *ciphertext* menggunakan kunci *b* yang berbeda yaitu, $C_1$ dengan $b_1$, $C_2$ dengan $b_2$ dan seterusnya, sehingga menghasilkan *plaintext* **Ini password yang digunakan: LFA@123ebfm.**

## Analisis Koefisien Korelasi

Pada tahap ini, dilakukan perhitungan untuk mencari nilai koefisien korelasi dari *affine cipher* dengan modifikasi kunci berdasarkan barisan Fibonacci. *Plaintext* yang digunakan dalam analisis koefisien korelasi sama dengan *plaintext* pada proses enkripsi Tabel 1. Sebelum dilakukan perhitungan *plaintext* dan *ciphertext* dikonversi terlebih dahulu ke bentuk desimal seperti Tabel 2. dan Tabel 4. Perhitungan nilai koefisien korelasi menggunakan persamaan (4). Hasil perhitungan nilai koefisien korelasi *affine cipher* dengan modifikasi kunci berdasarkan barisan Fibonacci adalah 0.0968. Karakter sembarang yang digunakan dalam kunci *b* apabila sudah dijumlah dan dimodulo 95, kunci *b* tersebut berada pada interval 0-94. Percobaan pada Tabel 5 menggunakan *plaintext* "Ini password yang digunakan: LFA@123ebfm" dan menggunakan kunci *b* dari interval 0-94. Pada Tabel 5 dikatakan tidak baik apabila nilai koefisien korelasi *affine cipher* dengan modifikasi kunci berdasarkan barisan Fibonacci lebih besar dari *affine cipher* dan dikatakan baik apabila nilai koefisien korelasi lebih kecil dari *affine cipher*. Seperti yang terlihat pada Tabel 5 terdapat 10 karakter yang menghasilkan nilai koefisien korelasi *affine cipher* dengan modifikasi kunci berdasarkan barisan Fibonacci lebih besar dari *affine cipher* dan terdapat 85 karakter yang menghasilkan nilai koefisien korelasi lebih kecil. Algoritma yang mempunyai nilai koefisien korelasi yang lebih kecil atau semakin mendekati nol merupakan algoritma dengan proses enkripsi yang lebih baik. Pada Tabel 4.5 menghasilkan 89% yang menunjukkan bahwa *affine cipher* dengan modifikasi kunci berdasarkan barisan Fibonacci lebih baik dari pada *affine cipher*. Hasil presentase dari percobaan tersebut tidak berlaku untuk *plaintext* yang lain.

Tabel 5. Hasil perbandingan nilai koefisien korelasi *Affine* Fibonacci

| **Jml** | B | TB | **Jml** | B | TB |
|---|---|---|---|---|---|
| **0-23** | √ | | **37** | √ | |
| **24** | | √ | **38** | | √ |
| **25** | √ | | **39** | | √ |
| **26** | | √ | **40** | √ | |
| **27** | √ | | **41** | | √ |
| **28** | | √ | **42** | √ | |
| **29** | √ | | **43** | √ | |
| **30** | | √ | **44** | | √ |
| **31-35** | √ | | **45-94** | √ | |
| **36** | | √ | | | |

Keterangan:

Jml : Total jumlah *plaintext* dimodulo 95
B : Baik ( Nilai koefisien korelasi lebih kecil )
TB : Tidak Baik ( Nilai koefisien korelasi lebih besar )

## 4. Kesimpulan

Berdasarkan hasil penelitian yang telah dilakukan, dapat disimpulkan sebagai berikut.

a. Proses enkripsi menggunakan *affine cipher* dengan modifikasi kunci berdasarkan barisan Fibonacci dapat menghilangkan kelemahan pada *affine cipher* yang hanya menggunakan kunci *b* sebanyak 1 karakter. *Ciphertext* yang dihasilkan terlihat acak dan tidak memiliki pola;

b. Hasil analisis yang telah dilakukan membuktikan bahwa proses enkripsi *affine cipher* dengan modifikasi kunci berdasarkan barisan Fibonacci lebih baik dari pada *affine cipher*;

c. Pembuatan program menggunakan *affine cipher* dengan modifikasi kunci berdasarkan barisan Fibonacci menggunakan *software* Matlab 2015a. Pembuatan program yang telah dilakukan memudahkan peneliti dalam poses enkripsi dan dekripsi.

## Daftar Pustaka

[1] Cahyono, J. (2016). Konstruksi Suatu Algoritma Kriptografi Menggunakan Transformasi Max Plus Wavelet. *Tesis.* Surabaya: Program Magister Fakultas Matematika dan Ilmu Pengetahuan Alam Institut Teknologi Sepuluh Nopember.

[2] Firdaus, I. L., Marati, R. dan Sispiyati, R. (2017). Aplikasi Kriptografi Komposisi One Time Pad Cipher dan Affine Cipher. *Eurekamatika* 5(2): 42-51.

[3] Prabhat, S. S dan Verma, K. (2014). Implementation of Affine Substitution Cipher with Keyed Transposition Cipher for Enhancing Data Security. *International Journal of Advanced Research in Computer Science and Software Engineering* 4(1): 237-238.

[4] Sharma, P., Bhatpahri, P. dan Shrivastava, R. (2018). Encryption of Hindi Plaintext Using Modified Affine Cipher Technique. *International Journal of Education and Information Technology* 3(4): 107-111.

[5] Sriramoju, A. B. (2017). Modification Affine Ciphers Algorithm for Cryptography Password. *International Journal of Research in Science & Engineering* 4(1): 2394-8299.

[6] Tung, K. Y. (2008). *Memahami Teori Bilangan dengan Mudah dan Menarik.* Jakarta: PT. Grasindo